# Robo de Identitad y "Phishing"
## (Identity Theft and Phishing)

*Mensaje para el Consumidor*

El gobierno federal reporta que el robo de identidad es el crimen de finanzas que está creciendo con más rapidez. Cada 79 segundos, un ladrón roba la identidad de una persona y abre una cuenta con el nombre de su víctima.
Para mejor proteger sus residentes en contra del robo de identidad, Nueva Jersey puso en efecto el Acta de Prevención de Robo de Identidad el 1º de Enero del 2006.

### LA LEY DE NUEVA JERSEY

- Requiere que las oficinas locales de policía tomen un reporte de usted si usted dice que ha sido una víctima de robo de identidad
- Permite que usted congele su reporte de crédito lo cual prohíbe a las agencias de reporte de crédito que den su reporte a una tercera parte sin su permiso.
- Requiere que entidades públicas destruyan los documentos suyos, si estos contienen información personal cuando los archivos se purgan.
- Requiere de negocios o entidades públicas que recogen o mantienen archivos computarizados los cuales tienen información personal, que notifiquen a los residentes de Nueva Jersey si alguna persona sin autorización ha hecho una brecha en el seguro de sus archivos computarizados; y
- Prohíbe a cualquier entidad pública o privada que ponga o publique su número de Seguro Social, imprima su número de Seguro Social en materiales mandados por correo o intencionalmente haga su número de Seguro Social disponible al público o transmitirlo a través del Internet a no ser que el número esté en clave.

### LOS CONSUMIDORES SE PUEDEN PROTEGER HACIENDO LO SIGUIENTE:

- Mantenga una lista de todos los números de cuentas incluyendo sus números de tarjetas de crédito y la fecha de caducidad, así como los números de teléfonos de sus acreedores.
- Revise cuidadosamente sus cuentas bancarias y mensuales para que no haya errores y póngase en contacto cons sus acreedores si cree que hay un error o si sus cuentas no llegan a tiempo.
- No responda a e-mail (correo electrónico) incluso cuando parece que viene del gobierno- que le pida información personal o de sus cuentas. En lugar, llame a la compañía o vaya a la web de ésta si sabe la correcta dirección de la red.
- No dé información personal por teléfono a los tele-mercaderes. Si usted desea comprar algo o contribuir a una caridad dígale que le manden información por correo.
- No dé su información de tarjeta de crédito a ninguna compañía por teléfono, a no ser que usted haya iniciado la llamada y tenga una relación de negocios con la compañía.
- Cuando compre artículos en el Internet, sólo dé su número de tarjeta de crédito después que ha establecido

sin duda alguna que el sitio web es legítimo y mantenido por una compañía en la que usted confía. Revise la Declaración de Privacidad del sitio web para determinar como usan su información personal.

- Si pierde o le han robado su cartera, tarjetas de crédito o cheques, cancelelos.
- Destruya todo lo que tenga identificación personal incluyendo los recibos de tarjeta de crédito.
- Destruya también las ofertas de crédito pre-aprobado que reciba por correo.

## "PHISHING"

Hay una estafa usada por los ladrones de robo de identidad llamada "phishing". Los ladrones atraen a sus víctimas con e-mails (correos electrónicos) disfrazados como avisos del gobierno, o llamadas telefónicas de una organización o compañía ilegítima que preguntan por su información personal como su tarjeta de crédito o cuenta de banco. La Liga Nacional de Consumidores (National Consumers League) dice que "phishing" es el cuarto timo más común en el Internet.

- Si usted recibe un correo electrónico o un mensaje instantáneo que pide por su información personal, no conteste.
- No mande por correo electrónico información personal o financiera. El e-mail no es una forma segura de transmitir información personal.
- Mire por indicaciones de que el sitio web es seguro. Mire por un icono (candado) o una dirección que empieza con "https" (la s quiere decir seguro)
- Llame a la organización para saber si el e-mail es legítimo.

## SI USTED CREE QUE HA SIDO VÍCTIMA DE ROBO DE IDENTIDAD

1. Ponga una alerta en su reporte de crédito llamando a las tres compañías de reporte de crédito listadas:

| | |
|---|---|
| **EQUIFAX** | 1-800-525-6285 |
| www.equifax.com | P.O. BOX 740241<br>Atlanta, GA 30374 |
| **Experian** | 1-888-397-3742 |
| www.experian.com | P.O. Box 9532<br>Allen, TX 75013 |
| **Trans Union** | 1-800-680-7289 |
| www.transunion.com | Fraud Victim Assistance<br>P.O. Box 6790<br>Fullerton, CA 92834 |

2. Cierre las cuentas que usted cree o sospecha que han sido manipulados, o cree, que han sido manipulados o abiertos engañosamente.

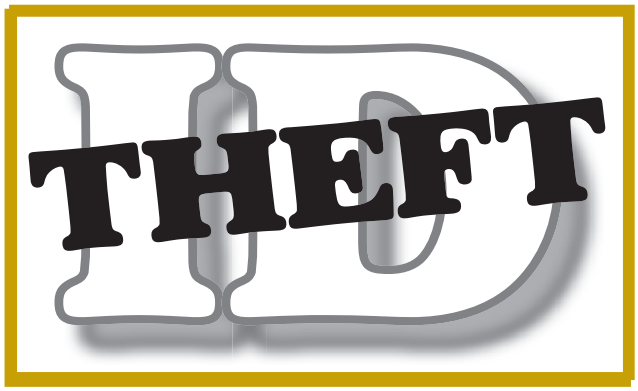
3. Haga un reporte con su policía local o la policía de su comunidad donde el robo de identidad tuvo lugar.

4. Vaya a **www.NJConsumer.Affairs.gov** para ponerse en contacto con la División de Asuntos del Consumidor del Estado de Nueva Jersey.

5. Vaya a **www.consumer.gov/idtheft** para fichar una queja con el Federal Trade Commission o F.T.C. (Comisión Federal de Comercio)

   Puede llamar a la F.T.C. gratis al 1-877-438-4338
   TDD (telecomunicaciones para sordo-mudos)
   202- 326-2502

   o puede escribir a:

   **Identity Theft Clearinghouse**
   **Federal Trade Commission**
   600 Pennsylvania Ave.
   NW, Washington, DC 20580

El número de teléfono gratis de la Clearinghouse es: 1-800-242-5846